УДК 004.056

Пфо О.М.
Кіровоградський національний технічний університет

Основні поняття і класифікація кіберзлочинності

Злочинність у віртуальному просторі – явище нове, але частина злочинів, скоєних у сфері високих технологій - це знайомі крадіжки, шахрайства, вимагання. І для дослідження проблеми кіберзлочинності необхідно дати коректні визначення таких явищ, як віртуальний простір, кіберзлочинність, комп'ютерні злочини, кібертероризм, щоб відмежувати їх один від одного і від суміжних понять.

Кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей. Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет. Киберзлочинічтю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, з метою видозміни комп'ютерних даних. При цьому комп'ютер виступає в якості предмета злочину, а інформаційна безпека об'єкта. До подій, пов'язаних зі злочином можна віднести ситуації, при яких комп'ютер – знаряддя для вчинення злочинів, з метою порушення авторських прав, громадської безпеки, прав власності, моральності. Класифікація кіберзлочинів:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

- незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;
- нелегальне перехоплення комп'ютерних даних;
- втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;
- втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;
- зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

У той же час, з урахуванням мотивації злочинців, кіберзлочини представляється можливим умовно розділити на наступні категорії: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини.

Перша категорія злочинів – привласнення грошових коштів, при якому шахраї використовують різні способи, іноді змушуючи

користувачів самостійно розкривати конфіденційні дані.

Найбільш поширені злочини, які відносяться до другої і третьої категорії – це злом баз даних і виведення з ладу комп'ютерних систем компаній і державних організацій, а також крадіжка інновацій або технологій.

В рамках даного дослідження найбільш докладно розглянуті кіберзлочини, в результаті яких виникає фінансова або інша матеріальна вигода у вигляді незаконно отриманих доходів. В першу чергу, мова йде про використання інформаційно-комунікаційних систем і комп'ютерних технологій для доступу до приватної власності юридичних і фізичних осіб та подальших дій по управлінню або розпорядження цією власністю. Зокрема, найбільш популярним на сьогодні серед кіберзлочинів є отримання доступу до засобів клієнтів банківських установ.

У цій категорії найбільш поширеними є наступні види злочинів:

1) шахрайство в мережі Інтернет, зокрема: створення «фінансових пірамід» в мережі Інтернет; шахрайство при продажу товарів (послуг) через Інтернет або на Інтернет-аукціонах; діяльність по створенню програмних засобів з метою розкрадання фінансової, комерційної або персональної інформації (створення фіктивних WEB-сайтів, поширення комп'ютерних вірусів і троянських програм, перехоплення трафіку тощо);

2) шахрайство в системах дистанційного банківського обслуговування (далі – ДБО), зокрема: створення комп'ютерних вірусів і троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО; відкриття рахунків, проведення несанкціонованих операцій і отримання готівкових коштів в результаті несанкціонованих операцій у системах ДБО; отримання платежів від іноземних відправників через міжнародну систему SWIFT внаслідок втручання в роботу комп'ютерів і систем ДБО клієнтів іноземних банківських установ.

3) підробка платіжних карток і банкоматне шахрайство, зокрема: використання втрачених/викрадених/підроблених платіжних карток; викрадення реквізитів платіжних карт, у тому числі із застосуванням технічних засобів їх «клонування»; скіммінг – виготовлення, збут і установка на банкомати пристроїв читання/копіювання інформації з магнітної смуги платіжної карти та отримання ПІН-коду до неї; використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах; Transaction Reversal Fraud – втручання в роботу банкомату при здійсненні операцій видачі готівки, яка залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; Cash Trapping – заклеювання диспенсера для присвоєння зловмисником готівки, яка була списана з карткового рахунки законного держателя картки.

Слід зазначити, що стрімкий розвиток сфери інформаційних технологій постійно генерує нові види послуг, у тому числі в фінансовій сфері. Це, в свою чергу, змушує злочинців удосконалювати свої здібності і придумувати нові способи незаконного заробітку в киберпросторі.

Список використаних джерел

1. *Tropina, T., Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds.), «Current Issues in ITU Security», Duncker & Humblot, Berlin, 2012.*
2. *Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // UNODC/CCPCJ/EG.4/2013/2.*
3. *Евпланов, А. Рунет: вне кризиса. Пользователи Интернета в России прирастут на треть // Российская газета. 2009. 19 мая.*